IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of: Burdett, Gregory; Mistry, Nalin; Fung, Bryant;

Serial No.	: **10/774,638**	Group Art Unit :	**2132**
Filed	: **July 2, 2002**	Examiner	: **Herring, Virgil A.**
For	: **Method and Apparatus for Accelerating CPE-based VPN Transmissions Over a Wireless Network**		
Date	: **September 18, 2008**	Docket No.	: **08894984US**

The Honorable Commissioner of Patents and Trademarks,
MAIL STOP APPEAL BRIEF - PATENTS
P.O. BOX 1450
ALEXANDRIA, VA22313-1450

SUBMISSION OF APPEAL BRIEF

Sir:

This Appeal is from the decision of the Patent Examiner dated March 21, 2008, rejecting claims 1-12, which are reproduced as (VIII) Claim Appendix in this Appeal Brief.

Please charge the $510.00 government fee to Deposit Account No. 50-1644.

Please charge any additional fee(s) that may be required by this paper or extension, and/or credit any overpayment to Deposit Account No. 50-1644.

Respectfully Submitted,

/Xiang Lu/

Xiang Lu
Registration No. 57,089

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of: Burdett, Gregory; Mistry, Nalin; Fung, Bryant;

Serial No.	: **10/774,638**	Group Art Unit	: **2132**
Filed	: **July 2, 2002**	Examiner	: **Herring, Virgil A.**
For	: **Method and Apparatus for Accelerating CPE-based VPN Transmissions Over a Wireless Network**		
Date	: **September 18, 2008**	Docket No.	: **08894984US**

The Honorable Commissioner of Patents and Trademarks,
MAIL STOP APPEAL BRIEF - PATENTS
P.O. BOX 1450
ALEXANDRIA, VA22313-1450

APPEAL BRIEF

Appellants hereby appeal to the Board of Patent Appeals and Interferences from the last decision of the Examiner.

(I) REAL PARTY IN INTEREST

The entire interest in the present application, and the invention to which it is directed, is assigned to Nortel Networks Limited, as recorded in the Patent and Trademark Office on Reel 021475, Frame 0516 on September 3, 2008.

(II) RELATED APPEALS AND INTERFERENCES

To the knowledge and belief of Appellants, the Assignee and the undersigned, there are no other appeals or interferences before the Board of Appeals and Interferences that will directly affect or be affected by the Board's decision in the instant Appeal.

(III) STATUS OF CLAIMS

Claims 1-12 are pending, all of which have been rejected. Thus, the rejections of claims 1-12 are appealed herein. A list of the claims on appeal is provided in (VIII) Claim Appendix.

(IV) STATUS OF AMENDMENTS

No amendments have been filed subsequent to the Final Rejection dated March 21, 2008.

(V) SUMMARY OF CLAIMED SUBJECT MATTER

This invention relates to method and apparatus for accelerating customer premises equipment-based virtual private network transmissions over a wireless network (*see* the present application, page 1, lines 6-7).

Independent claim 1 recited a method of securely accelerating customer premises equipment based virtual private network (*see* the present application, page 2, lines 12-13) transmissions over a carrier network (*see* the present application, page 7, lines 9-10) comprising the steps of: establishing an encrypted acceleration tunnel between a VPN acceleration client and a VPN acceleration server (*see* the present application, page 8, lines 13-14) in response to a VPN acceleration client request for information (*see* the present application, page 8, line 22), the encrypted acceleration tunnel traversing a wireless network (*see* the present application, page 8, lines 20-21, Figure 4, numeral 162); transmitting said VPN acceleration client's address and required data information (*see* the present application, page 9, lines 12-14) to said VPN acceleration server over said encrypted acceleration tunnel (*see* the present application, page 9, lines 12-14); establishing a VPN tunnel between said VPN acceleration server and a VPN switch (*see* the present application, page 8,

lines 14-16; page 10, lines 15-17 and numeral 164 in Figure 4), said VPN switch accessing a plurality of enterprise content servers (*see* the present application, page 7, lines 18-21), said plurality of enterprise content servers providing said required data information transmitted (*see* the present application, page 7, line 21 to page 9, line 2), wherein said encrypted acceleration tunnel and said VPN acceleration server utilize the same network layer in a standard OSI model (*see* the present application, page 3, line 15 to page 4, line 19); communicating required data responding to said required data information from one of said plurality of enterprise content servers to said VPN switch (*see* the present application, page 9, line 18 to page 10, line 2); transmitting said required data from said VPN switch to said VPN acceleration server over said VPN tunnel (*see* the present application, page 10, lines 3-7); accelerating and encrypting said required data using wireless communication performance optimization by said VPN acceleration server (*see* the present application, page 10, lines 8-10); transmitting said required data to said VPN acceleration client (*see* the present application, page 10, line 9); and decrypting said required data in response to said VPN acceleration client (*see* the present application, page 10, lines 8-10) receiving said required data.

Independent claim 7 recited a VPN acceleration server (*see* the present application, page 8, lines 3-5) comprising: a first module for terminating a virtual private network (VPN) tunnel (*see* the present application, page 8, lines 14-15 and page 9, lines 18-19) to a VPN switch (*see* the present application, page 8, lines 14-16 and page 9, line 19), said VPN switch accessing a plurality of enterprise content servers (*see* the present application, page 7, lines 18-21), said plurality of enterprise content servers providing required data information (*see* the present application, page 7, line 21 to page 9, line 2); a second module for accelerating data for transmission over a wireless network using wireless communication performance optimization (*see* the present application, page 10, line 9, and page 11, lines 8-10); and a third module for terminating an encrypted acceleration tunnel to a wireless client whereby a secure virtual network service is provided between the VPN switch and the wireless client, for

which acceleration of data on the wireless network is provided (*see* the present application, page 10, lines 8-10), wherein said encrypted acceleration tunnel and said virtual private network tunnel utilize the same network layer in a standard OSI model (*see* the present application, page 3, line 15 to page 4, line 19).

(VI) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1 to 12 were rejected under 35 U.S.C. §103(a) as being unpatentable over Travaly et al. (US Publication 2002/0159441), hereinafter referred as Travaly.

(VII) ARGUMENT

Appellants respectfully submit that claims 1 to 12 are inventive over Travaly.

Appellants respectfully submit that the rejections of Appellants' claims in the Final Office Action mailed March 21, 2008, hereinafter referred to as Office Action, are clearly based on errors, and omit essential elements required to establish a *prima facie* §103 rejection, as set forth below:

Encrypted acceleration tunnel not a VPN

The Examiner interprets the claimed encrypted acceleration tunnel, which traverses a wireless network, and is between a VPN acceleration client and a VPN acceleration server, as a VPN tunnel (*See* Office Action, page 3, last paragraph, page 5; last paragraph; page 6, second and last paragraphs; and page 8, first full paragraph).

This is not correct.

As stated throughout the disclosure, for example at page 11, lines 10 to 13, "Given that the VPN tunnel is only established over the Internet, and not over the Air Interface of the wireless network one can ensure VPN permanence as the problem of dropped VPN connections due to coverage issues, is avoided" [emphasis added]

Furthermore, it should be clear to a person skilled in the art when reading the present specification, and for example, comparing Figure 1 (prior art) and Figure 4, that the VPN tunnel (164) is only between the VPN acceleration server (160) and the VPN switch (112). *See* Figure 4, and page 8, lines 13-16; page 9, lines 10-12; page 10, lines 15-16; and page 11, lines 10-13 of the present application.

Appellants respectfully note that it has been judicially determined that where an explicit definition is provided by the applicant for a term, that definition will control interpretation of the term as it is used in the claim. *Toro Co. v. White Consolidated Industries Inc.*, 199 F.3d 1295, 1301, 53 USPQ2d 1065, 1069 (Fed. Cir. 1999). Further, the meaning of a particular claim term may be defined by implication, that is, according to the usage of the term in the context in the specification. *Phillips v. AWH Corp.*, 415 F.3d 1303, 75 USPQ2d 1321 (Fed. Cir. 2005) (en banc); and *Vitronics Corp. v. Conceptronic Inc.*, 90 F.3d 1576, 1583, 39 USPQ2d 1573, 1577 (Fed. Cir. 1996).

Therefore, the Examiner's rejections based on the mistaken assumption are improper.

Encrypted acceleration tunnel traversing a wireless network

The claimed method of the present application includes "establishing an encrypted acceleration tunnel between a VPN acceleration client and a VPN acceleration server [...] the encrypted acceleration tunnel traversing a wireless network". This acceleration tunnel, as discussed in the above, is a non VPN

tunnel and utilizes various wireless communication performance optimization techniques including compression, protocol optimization, caching, and traffic management. See page 3, lines 7-10; page 8, lines 7-9 of the present application; and claim 12. Therefore, it should be abundantly clear to a person skilled in the art that acceleration refers to wireless communication performance optimization.

Travaly includes a VPN Accelerator 54, located between a VPN router 56 and an Ethernet hub 120 in Figure 5. However, there is no indication as to what the VPN Accelerator is or does. In fact, there is no description of numeral 54 in Travaly. There is no reason for a person skilled in the art to read this VPN Accelerator 54 as an accelerator for a wireless network, i.e. performing wireless communication performance optimization, because VPN Accelerator 54 of Travaly does not even interface the wireless network. Therefore, Travaly does not teach or suggest an "encrypted acceleration tunnel traversing a wireless network".

The Examiner stated that "because the system as a whole is a computer network employing VPN and wireless technology" (page 2, last paragraph of the Office Action), and interpreted that VPN Accelerator 54 and client 116 or 118 of Travaly as "establishing an encrypted acceleration tunnel between a VPN acceleration client and a VPN acceleration server in response to a VPN acceleration client request for information, the encrypted acceleration tunnel traversing a wireless network" (page 5, second last paragraph of the Office Action).

Appellants note that this "as a whole" inquiry is improper.

The subject matter of Travaly, as a whole, is directed to digitization of work processes through the use of a wireless network with user wearable end devices. Specifically, Travaly describes a system for digitization of work

processes in a power plant having a gas turbine including a processor system with a controller.

Travely is not concerned about the problem of "[one] of the major drawbacks [in prior art CPE-VPN] ... to utilize various wireless communication performance optimization techniques including compression, protocol optimization, caching, and traffic management" (*see* page 3, lines 6-9 of the present application), and therefore does not provides a solution of establishing VPN tunnel only "over the Internet, and not over the Air Interface of the wireless network one can ensure VPN permanence as the problem of dropped VPN connections due to coverage issues, is avoided" (*see* page 11, lines 10-13 of the present application).

Appellants note that "[A] patentable invention may lie in the discovery of the source of a problem even though the remedy may be obvious once the source of the problem is identified. This is part of the 'subject matter as a whole' which should always be considered in determining the obviousness of an invention under 35 U.S.C. § 103." *In re Sponnoble*, 405 F.2d 578, 585, 160 USPQ 237, 243 (CCPA 1969). (emphasis added)

communicating required data responding to said required data information from one of said plurality of enterprise content servers to said VPN switch

As claimed, a request (required data information) is sent from the VPN acceleration client. The required data responding to the request is communicated from one of the enterprise content servers, first to the VPN switch, then to the VPN acceleration server, and accelerated and encrypted by the VPN acceleration servers using wireless communication performance optimization.

The Examiner asserted that "[a]ny server is a 'content server', and the 'enterprise content' .... is application data or web portal data". Even if this interpretation were correct, which it is not, Travaly failed to teach or suggest the

claimed request/response type limitation between the VPN acceleration client and the enterprise content server.

Furthermore, Appellants submit that the Supreme Court in *KSR International Co. v. Teleflex Inc.,* 550 U.S. ___, 82 USPQ2d 1385, 1396 noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit. The Court quoting *In re Kahn,* 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006), stated that "'[R]ejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.'" KSR, 550 U.S. at ___, 82 USPQ2d at 1396.

accelerating and encrypting said required data using wireless communication performance optimization by said VPN acceleration server

The Examiner stated that this limitation was inherent. *See* Office Action, page 6, last paragraph.

As claimed, the encrypted acceleration tunnel traversing the wireless network is established between the VPN acceleration server and the VPN acceleration client, and the required data is transmitted to the VPN acceleration client after acceleration and encryption at the VPN acceleration server.

The claimed limitation is not inherent.

Inherency

The Examiner used inherency as the ground for rejection in many instances in the Office Action, (page 5 last paragraph; page 6, 2nd, 5th, and 6th paragraphs; page 7, 5th paragraph; and page 8, last paragraph).

The fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.' " *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999). "In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art." *Ex parte Levy*, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990).

Claimed embodiment non-obvious

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In *re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." In *re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). The Examiner has not met his burden as at least the foregoing elements of the claim are not taught or suggested by the prior art.

Rejection based on assertions that a fact is well-known is not judiciously applied

The Examiner stated that the limitations of encryption and acceleration "over a network via a VPN" in claims 1 and 7 were well known. *See* Office Action, page 7, last paragraph.

As discussed above, the claimed encrypted acceleration tunnel is not a VPN channel.

Should the Examiner consider that the rejection applies to a non-VPN encrypted acceleration tunnel, Appellants respectfully note that any rejection based on assertions that a fact is well-known or is common knowledge in the art without documentary evidence to support the examiner's conclusion should be judiciously applied. The examiner's rejection based on assertions that a fact is well-known is not judiciously applied.

Conclusion

Appellants have demonstrated that the present invention as claimed is clearly distinguishable over the art cited of record. Therefore, Appellants respectfully request the Board of Patent Appeals and Interferences to reverse the rejection of the Examiner, issued on March 21, 2008, and instruct the Examiner to issue a notice of allowance of all claims.

(VIII) CLAIM APPENDIX

The Appealed Claims:

1. A method of securely accelerating customer premises equipment based virtual private network transmissions over a carrier network comprising the steps of:

establishing an encrypted acceleration tunnel between a VPN acceleration client and a VPN acceleration server in response to a VPN acceleration client request for information, the encrypted acceleration tunnel traversing a wireless network;

transmitting said VPN acceleration client's address and required data information to said VPN acceleration server over said encrypted acceleration tunnel;

establishing a VPN tunnel between said VPN acceleration server and a VPN switch, said VPN switch accessing a plurality of enterprise content servers, said plurality of enterprise content servers providing said required data information transmitted, wherein said encrypted acceleration tunnel and said VPN acceleration server utilize the same network layer in a standard OSI model;

communicating required data responding to said required data information from one of said plurality of enterprise content servers to said VPN switch;

transmitting said required data from said VPN switch to said VPN acceleration server over said VPN tunnel;

accelerating and encrypting said required data using wireless communication performance optimization by said VPN acceleration server;

transmitting said required data to said VPN acceleration client; and

decrypting said required data in response to said VPN acceleration client receiving said required data.

2. A method as claimed in claim 1 wherein the step of establishing an encrypted acceleration tunnel uses public key infrastructure (PKI) encryption.

3. A method as claimed in claim 1 wherein the required data information includes at least one of a VPN switch address, user name, and password.

4. A method as claimed in claim 1 wherein the encrypted VPN tunnel is an IPSec tunnel.

5. A method as claimed in claim 1 wherein the encrypted VPN tunnel is an MPLS tunnel.

6. A method as claimed in claim 1 wherein the encrypted VPN tunnel is a L2TP tunnel.

7. A VPN acceleration server for providing secure virtual private network service for wireless clients comprising:

a first module for terminating a virtual private network (VPN) tunnel to a VPN switch, said VPN switch accessing a plurality of enterprise content servers, said plurality of enterprise content servers providing required data information;

a second module for accelerating data for transmission over a wireless network using wireless communication performance optimization; and

a third module for terminating an encrypted acceleration tunnel to a wireless client whereby a secure virtual network service is provided between the VPN switch and the wireless client, for which acceleration of data on the wireless network is provided, wherein said encrypted

acceleration tunnel and said virtual private network tunnel utilize the same network layer in a standard OSI model.

8. A server as claimed in claim 7 wherein the virtual private network tunnel is IPSec.

9. A server as claimed in claim 7 wherein the virtual private network tunnel is MPLS.

10. A server as claimed in claim 7 wherein the virtual private network tunnel is L2TP.

11. A server as claimed in claim 7 wherein the encrypted tunnel is public key infrastructure encrypted.

12. A method as claimed in claim 1, wherein the wireless communication performance optimization is selected from a group consisting of compression, protocol optimization, caching, traffic management and a combination thereof.

(IX) EVIDENCE APPENDIX

None

(X) RELATED PROCEEDINGS APPENDIX

None

Respectfully Submitted,

/Xiang Lu/

Xiang Lu
Reg No. 57,089

c/o GOWLING LAFLEUR HENDERSON LLP
160 Elgin Street, Suite 2600
Ottawa, Ontario
K1P 1C3
CANADA

Telephone: (613) 233-1781
Facsimile: (613) 563-9869